堡垒机的功能：

在实际应用中堡垒机又被称为“堡垒主机”，是一个主机系统，其自身通常经过了一定的加固，具有较高的安全性，可抵御一定的攻击，其作用主要是将需要保护的信息系统资源与安全威胁的来源进行隔离，从而在被保护的资源前面形成一个坚固的“堡垒”，并且在抵御威胁的同时又不影响普通用户对资源的正常访问。

运维审计型堡垒机被部署在内网中的服务器和网络设备等核心资源的前面，对运维人员的操作权限进行控制和操作行为审计;运维审计型堡垒机即解决了运维人员权限难以控制混乱局面，又可对违规操作行为进行控制和审计，而且由于运维操作本身不会产生大规模的流量，堡垒机不会成为性能的瓶颈，所以堡垒机作为运维操作审计的手段得到了快速发展。

运维操作审计手段的堡垒机的核心功能是用于实现对运维操作人员的权限控制与操作行为审计。

堡垒机核心功能：

单点登录功能

支持对X11、linux、unix、数据库、网络设备、安全设备等一系列授权账号进行密码的自动化周期更改，简化密码管理，让使用者无需记忆众多系统密码，即可实现自动登录目标设备，便捷安全。

账号管理

设备支持统一账户管理策略，能够实现对所有服务器、网络设备、安全设备等账号进行集中管理，完成对账号整个生命周期的监控，并且可以对设备进行特殊角色设置如：审计巡检员、运维操作员、设备管理员等自定义设置，以满足审计需求

身份认证

设备提供统一的认证接口，对用户进行认证，支持身份认证模式包括 动态口令、静态密码、硬件key 、生物特征等多种认证方式，设备具有灵活的定制接口，可以与其他第三方认证服务器之间结合；安全的认证模式，有效提高了认证的安全性和可靠性。

资源授权

设备提供基于用户、目标设备、时间、协议类型IP、行为等要素实现细粒度的操作授权，最大限度保护用户资源的安全

访问控制

设备支持对不同用户进行不同策略的制定，细粒度的访问控制能够最大限度的保护用户资源的安全，严防非法、越权访问事件的发生。

操作审计

设备能够对字符串、图形、文件传输、数据库等全程操作行为审计；通过设备录像方式实时监控运维人员对操作系统、安全设备、网络设备、数据库等进行的各种操作，对违规行为进行事中控制。对终端指令信息能够进行精确搜索，进行录像精确定位。[3]